UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,145	06/14/2001	Craig Partridge	BBNT-P01-368	8070

28120 7590 08/16/2007
FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
TIV, BACKHEAN	

ART UNIT	PAPER NUMBER
2151	

MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	09/881,145	PARTRIDGE ET AL.
	Examiner	Art Unit
	Backhean Tiv	2151

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *RCE filed on 5/29/07*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-20* is/are pending in the application.

4a) Of the above claim(s) *11,12,21-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Detailed Action

Claims 1-10, 13-20 are pending in this application. Claims 11,12,21,22,25 have been withdrawn from consideration. Claims 23,24 have been cancelled. This is a response to the RCE filed on 5/29/07.

Claim Objections

Claim 1 is objected to because of the following informalities:

As per claim 1, last line, there should be a period after encountered, and not a comma.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 7, 9, 10, 13-15, 17, 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,991,881 issued to Conklin et al. (Conklin) in view of US Patent No. 6,389,419 issued to Wong et al. (Wong) in further view of US Patent 6,279,113 issued to Vaidya.

As per claim 1, Conklin discloses in a network carrying a plurality of packets over at least one network link, said network including a computer, a first network component having memory and a processor and configured to store information in said memory about at least one of said plurality of packets to locate an intrusion point of a target packet, wherein said target packet is a respective one of said plurality of packets and a second network component (fig. 16), a method for detecting target packet comprising (col. 1 L10-65): receiving said at least one of said plurality of packets over a link to obtain a received packet (fig. 7, fig. 8, col. 3 L60-65); receiving a query message identifying a target packet at said first component (fig. 7, fig. 8, col. 3 L1-14); creating a reply if said target packet has been encountered (col. 4 L9-60, col. 5 L10-60, fig. 6, fig. 9); and said first network component making said reply available to said network if said target packet has been encountered, wherein reply is capable of being used as part of a method for locating said intrusion point for said first one of the packets (fig. 9),

However, Conklin does not disclose the process of determining a hash value of at least a portion of said packet; using said has value to identify a location in a memory; setting a flag in said memory, said flag associated with said location; and said first network component using a flag in processing said query message to determine if said target packet has previously been received and/or encountered (note that Conklin teaches the process of detecting an intrusion by pattern matching or comparing, see col. 7 L50-65, fig. 7).

Wong, from the same field of endeavor explicitly discloses the process of determining a hash value of at least a portion of said packet (fig. 2B item #222, fig. 2C item #242 and fig. 3C, fig. 6 item #602, col. 6 L4-8); using said hash value to identify a location in a memory (fig. 2B item #224, fig. 2C item #244, fig. 6 item #604); setting a flag in said memory, said flag associated with said location (fig. 6 item #608, fig. 8 item

#818820, 822, col. 6 L4-15, col. 7 L28-36, col. 9 L6-33); and said first network component using a flag in processing said query message (a message or a packet) (fig. 8 item #818, 820, 822 and fig. 6 item #608, 610, col. 5 L59-63, col. 6 L4-36).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to use the hashing technique to determine or identify the packet.

One of ordinary skilled in the art would have been motivated because it would have located and/or identified the packet (whether target, incoming or outgoing) in a more efficient manner, which would have reduced the latency in the network appliance (Wong, col. 2 L19-41, col. 3 L27-30, L45-51).

Conklin in view of Wong does not explicitly teach determining if said target packet has previously been received and/or encountered.

Vaidya teaches determining if a packet has previously been received and/or encountered(Abstract, col.3, lines 12-39, col.8, lines 16-39).

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention to modify the teachings of Conklin in view of Wong to explicitly determine if a packet has been received and/or encountered as taught by Vaidya in order to detect intrusion attempts into a system(Vaidya, col.1, lines 10-15).

One ordinary skill in the art at the time of the invention would have been motivated to combine the teachings of Conklin, Wong, and Vaidya in order to detect intrusion attempts into a system(Vaidya, col.1, lines 10-15).

As per claim 2, the process wherein making said reply available to said network includes forwarding said reply to said second network component(Conklin, fig. 9, col. 5 L10-60).

As per claim 3, the process wherein said second network component is a computer (Conklin, fig. 9, col. 5 L10-60).

As per claim 4, the process wherein said reply contains a network address for said first network component (Conklin, col. 6 L9-15).

As per claim 5, Conklin does not disclose the process wherein hash value is determined over the entire packet.

Wong, from the same field of endeavor discloses the process wherein the addresses in a packet are hashed (col. 5 L60 to col. 6 L35, fig. 2, fig. 5 and fig. 7-8).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in order to determine the hash value over the entire packet.

One of ordinary skilled in the art would have been motivated because of the same reasons as set forth in claim 1.

As per claim 7, the process wherein said network is an Internet Protocol (IP) network (Conklin, fig. 1)

As per claim 9, the process wherein said first network component is a router (Conklin, fig. 1-3).

As per claim 14, the system wherein said first interface and second interface are combined into a single bi-directional interface (Conklin, fig. 4).

As per claim 15, the process wherein said reply is made available to another network (Conklin, fig. 9).

As per claim 19, the combination of Conklin and Wong discloses the system wherein said reply is positive reply if said second has value matches at least one of said plurality of first hash values(Conklin, col.5, lines 60-col.6, line 35, Wong, col.6, lines 4-67).

As per claim 20, the system wherein said reply is forwarded to those of said devices one hop away (Conklin, fig. 9 and fig. 3).

As per claims 10, 13 and 17, they do not teach or further define over the limitations in claims 1-5, 7, 9, 14-15, 19 and 20. Therefore claims 10, 13 and 17 are rejected for the same reasons as set forth in claims 1-5, 7, 9, 14-15, 19 and 20.

Claims 8, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,991,881 issued to Conklin et al. (Conklin) in view of US Patent No. 6,389,419 issued to Wong et al. (Wong) in further view of US Patent 6,279,113 issued to Vaidya and further in view of “Official Notice”.

As per claim 8, Conklin in view of Wong in further view of Vaidya does not explicitly disclose the process wherein the link is a wireless link or network.

But, wireless networks and/or links are well known in the relevant art.

Official Notice is taken in order to indicate that the subject matter is in fact well known and obvious in the art.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in further view of Vaidya in order to implement the invention in wireless networks.

One of ordinary skilled in the art would have been motivated because wireless networks are very well known in the art and does not limit the system to wired networks.

As per claim 18, Conklin in view of Wong in further view of Vaidya does not explicitly disclose a system wherein the processor is an ASIC processor.

But, ASIC processors are simply well known and obvious in the relevant art.

Official Notice is taken to indicate that the ASIC processors are known and obvious in the art.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Conklin in view of Wong in further view of Vaidya in order to include ASIC processors.

One of ordinary skilled in the art would have been motivated because ASIC processors are simply known in the art.

As per claim 16, it does not teach or further define over the limitations in claim 8 and 18. Therefore claim 16 is rejected for the same reasons as set forth in claim 8 and 18.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 5,991,881 issued to Conklin et al. (Conklin) in view of US Patent No.

6,389,419 issued to Wong et al. (Wong) in further view of US Patent 6,279,113 issued to Vaidya further view of US Patent No. 6,842,861 issued to Cox et al. (Cox).

As per claim 6, Conklin in view of Wong in further view of Vaidya does not teach the process of determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time.

Cox teaches determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time (col.2, L 34-41).

Therefore it would have been obvious to one ordinary skilled in the art at the time of the invention to modify the teaching of Conklin in view of Wong in further view of Vaidya to add determining if said received packet has undergone a transformation, such transformation having occurred if a first hash value of at least a portion of said packet computed at a first time is not equal to a second hash value of at least a portion of said packet computed at a second time, said second time occurring after said first time as taught by Cox in order to determine infected files (Cox, col. 2, line 34).

One ordinary skilled in the art at the time of the invention would have been motivated to combine Cox, Wong, Conklin, Vaidya in order to provide a system to detect a file with a virus (Cox. col.1, lines 5-67).

Response to Arguments

Applicant's arguments with respect to claims 1-10, 13-20 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in its entirety as potentially teaching of all or part of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Backhean Tiv whose telephone number is (571) 272-5654. The examiner can normally be reached on M-F 6:30-3:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Valencia Wallace can be reached on (571) 272-3440. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BackheanTiv
2151
8/8/07

V. Martin Wallace

VALENCIA MARTIN-WALLACE
PRIMARY EXAMINER